



U.S. Department of Justice

*United States Attorney
Eastern District of New York*

HDM:MED
F. #2020R00093

*271 Cadman Plaza East
Brooklyn, New York 11201*

September 10, 2021

By ECF and Email

Honorable LaShann DeArcy Hall
United States District Judge
Eastern District of New York
225 Cadman Plaza East
Brooklyn, New York 11201

Re: United States v. Ashraf Omar Eldarir
Criminal Docket No. 20-243 (LDH)

Dear Judge DeArcy Hall:

The government respectfully writes in response to the defendant's opposition to the government's motion to preclude his proposed forensic expert at the evidentiary hearing scheduled in the above-referenced case for October 1, 2021. For the reasons discussed below, the Court should preclude the defendant's proposed forensic expert because suppression of the phone is not warranted as a matter of law even if all factual inferences are resolved in the defendant's favor.

I. Suppression is Not Warranted Even if Law Enforcement Searched the Defendant's Cell Phone Without a Warrant or Probable Cause

The defendant asserts that a forensic expert is necessary for the Court to determine whether (1) the phone was in airplane mode at the time of the manual search; and (2) a forensic search was conducted prior to the warrant. But neither of these issues have any bearing on suppression. That is, even assuming *arguendo* that the manual search was not permissible and a forensic search occurred prior to obtaining a warrant, suppression of the phone would not follow.¹

¹ The defendant asserts that the cell phone was forensically searched prior to obtaining a warrant. Def. Op. at 2. The government has conferred with HSI and informs the Court that the phone was imaged prior to obtaining a warrant on January 23, 2020, but its contents were not searched until after the warrant, sought in an abundance of caution, was obtained. The only evidence from the phone relied on in the search warrant affidavit is the photos viewed during the manual search of the phone at the border.

A. Legal Standard

It is well established in the Second Circuit that routine border searches do not require any suspicion whatsoever. Tabbaa v. Chertoff, 509 F.3d 89, 97–98 (2d Cir. 2007); see also United States v. Charleus, 871 F.2d 265, 267–68 (2d Cir. 1989) (“routine” border searches include searches of personal belongings, such as luggage); United States v. Borello, 766 F.2d 46, 58–59 (2d Cir. 1985) (“[T]he opening of the cartons and the screening of the films were plainly permissible steps in a reasonable border search.”). Non-routine searches are valid “if [they are] supported by reasonable suspicion.” United States v. Irving, 452 F.3d 110, 124 (2d Cir. 2006).

While the Second Circuit has not weighed in on whether a manual search of a cell phone at the border is routine or non-routine, several circuits to have considered the issue have held that such a search is routine, requiring no suspicion whatsoever. See, e.g., Alasaad v. Mayorkas, 988 F.3d 8, 18 (1st Cir. 2021); United States v. Cano, 934 F.3d 1002, 1015 (9th Cir. 2019) (manual searches require no suspicion “whatsoever”); United States v. Touset, 890 F.3d 1227, 1233 (11th Cir. 2018) (requiring no suspicion for border *forensic* search of electronic device); United States v. Kolsuz, 890 F.3d 133, 146 n.5 (4th Cir. 2018) (stating that United States v. Ickes, 393 F.3d 501 (4th Cir. 2005) treated a manual search of a computer as a routine border search, requiring no individualized suspicion for the search).

Further, no court has held that a forensic search of electronics at the border requires more than reasonable suspicion.² See United States v. Wanjiku, 919 F.3d 472, 485 (7th Cir. 2019) (“no circuit court, before or after Riley, has required more than reasonable suspicion for a border search of cell phones”). And no court in this Circuit has adopted the reasoning of United States v. Cano, 934 F.3d 1002, 1019 (9th Cir. 2019), which, apart from failing to appreciate the range of justifications underlying the border search exception, by its own terms would still allow a suspicionless manual search of a phone’s camera roll—unquestionably an area where digital contraband is likely to be stored.

Moreover, several courts in this Circuit, in denying motions to suppress, have found that border searches of electronics are routine searches that can be conducted with no suspicion whatsoever. See United States v. Jenkins, No. 5:11-CR-0602 (GTS), 2013 WL 12204395, at *2 (N.D.N.Y. Dec. 12, 2013) (citing Supreme Court precedent and noting that a forensic examination of an electronic device can be a routine search unless it is destructive of the

² The defendant cites United States v. Laich, No. 8-CR-20089 (JAC), 2010 WL 259041 (E.D. Mich. Jan. 20, 2010) in support of his argument that a border search of electronics must be supported by a warrant and probable cause. The defendant’s reliance on Laich is misplaced, as Laich dealt with a passenger whose laptop was detained and forensically search *after* he cleared Customs and was thus in the “extended border search” context. “The subsequent detention and forensic inspection of [Laich’s] laptop was therefore not a border search, and thus not governed by the border search doctrine.” United States v. Feiten, No. 15-CR-20631 (RHC), 2016 WL 894452, at *3 (E.D. Mich. Mar. 9, 2016) (finding Laich inapplicable in the border search context).

device or carried out in a “particularly offensive manner”); United States v. Dattmore, No. 12-CR-166A (RJA), 2013 WL 4718614, at *4 (W.D.N.Y. Sept. 3, 2013) (searches of electronic devices are routine searches that may be conducted without reasonable suspicion); United States v. Young, No. 12-CR-210 (RJA) (JJM), 2013 WL 885288, at *2–3 (Jan. 16, 2013 W.D.N.Y.) (declining to hold an evidentiary hearing and denying motion to suppress cell phones searched pursuant to the border search authority and later a warrant and noting that at most, reasonable suspicion was required); see also United States v. Jean Carlo Mano, No. 18-CR-367 (WFK), ECF No. 26 at 15 (May 9, 2019 Decision & Order) (denying motion to suppress statements disclosing passcodes and electronic devices and declining to determine what level of suspicion was required for a forensic border search of defendant’s electronics, finding that reasonable suspicion existed); United States v. Singh, No. 12-CR-121 (DLI), 2012 WL 2501032, at *3 (E.D.N.Y. June 27, 2012) (declining to address whether CBP’s search and duplication of the defendant’s cell phone was invasive which would render the search non-routine and finding that the search was supported by reasonable suspicion); United States v. Ighodaro, No. 10-CR-351 (RJA) (JJM), 2012 WL 5373453, at *7 (W.D.N.Y. July 5, 2012) (finding reasonable suspicion existed and declining to address whether search of cell phones was routine or non-routine); People v. Perkins, 126 N.Y.S.3d 745, 748, leave to appeal denied, 35 N.Y.3d 1115 (2020) (noting that “no court has required a warrant or probable cause for either a manual or forensic search of an electronic device for contraband at the border” and declining to determine the appropriate level where law enforcement had reasonable suspicion that contraband would be found on the defendant’s iPad).

B. Discussion

As discussed *supra*, Second Circuit law was clear at the time of the warrant that border searches of a passenger’s belongings require at most reasonable suspicion. Thus, even if the Court were to find, for the first in this Circuit, that a warrant was required for a border search of the defendant’s phone—manual or forensic—the good faith exception to the exclusionary rule would bar suppression of the phone. See United States v. Leon, 468 U.S. 897, 922 (1984).

Here, law enforcement had abundant reasonable suspicion that the defendant was engaged in criminal activity, including (1) information that the defendant had been selling Egyptian antiquities of suspicious provenance dating back to at least 2013; (2) a false Customs declaration filled out by the defendant that day declaring goods valued at \$300 and stating that he was not bringing any artifacts into the country; (3) the presence of over 500 artifacts—some smelling of wet earth and covered in loose sand and dirt—in the defendant’s luggage; (4) numerous papers reflecting sales and commissions of historic artifacts purporting to be in the United States since the 1940s by the defendant through various art galleries; (5) blank paper matching the style of provenances in the defendant’s luggage; and (6) loose stamps that appeared to be franked. Similarly, as argued *infra*, to the extent the Court finds that the manual search of the defendant’s phone was not permissible, at most such a finding would result in the excision of the photos from the warrant, which would still be supported by probable cause.

II. Suppression is Not Warranted Even if the Defendant's Phone was Not in Airplane Mode Before it was Manually Searched

The defendant also asserts that an alleged failure to follow CBP policy and place a phone in airplane mode renders the border search exception inapplicable. Even assuming that the phone was not in airplane mode at the time it was manually searched, suppression would not follow.³

The issue here is whether the WhatsApp photos law enforcement found on the camera roll during the manual search and relied upon as part of its probable cause showing in the warrant came across the border with the defendant on his phone when he entered the United States on January 22, 2020, or whether the photos were on an external server and accessed via cloud computing. It is well-settled law that an individual has a limited privacy right in items brought across the United States' international border. See United States v. Montoya de Hernandez, 473 U.S. 531, 539–40 (1985) (“[N]ot only is the expectation of privacy less at the border than in the interior, the Fourth Amendment balance between the interests of the Government and the privacy right of the individual is also struck much more favorably to the Government at the border.”). The defendant uses “airplane mode” as a proxy for this argument, contending that if the phone was not in airplane mode at the time of the manual search, there is a possibility that the photos in question were pulled from an external server and thus, according to the defendant's reasoning, did not come across the border with the defendant on his phone, rendering the border search exception null.

The defendant's argument, however, has no merit. Even assuming *arguendo* that the phone was not in “airplane mode” during the manual search and the WhatsApp photos on the defendant's phone were pulled from a remote server each time one was viewed during the phone's manual search at the border, the warrant still stands, as (1) the photographs were just one factor of many that Judge Mann relied on in issuing the warrant, (2) the application of United States v. Laynes, 481 F. Supp. 3d 657 (S.D. Ohio 2020) would not mandate suppression of evidence obtained pursuant to a warrant, and (3) the defendant has not, and cannot, make the

³ In consultation with HSI, based on the forensic report, the government is unable to conclusively determine whether and when the phone was placed into airplane mode, which can be overridden by default by a user's Wi-Fi and Bluetooth settings. The government is able to determine, however, that the last time the phone connected to Wi-Fi was in Cairo, Egypt, the defendant's place of departure, and that the last photograph received via WhatsApp automatically saved on the phone's camera roll, but is unable to determine whether automatic saving was disabled on the defendant's phone (which was returned to the defendant on February 20, 2020). “By default, photos and videos receive[d] through WhatsApp will automatically be saved in the WhatsApp folder of your iPhone's Photos.” <https://faq.whatsapp.com/iphone/how-to-save-incoming-media>. The government is unable to determine the last time the phone connected to a cellular network. Additionally, while Officer Hernandez cannot recall the specific act of toggling a phone into airplane mode on January 22, 2020, he has no reason to believe that he did not place the phone into airplane mode before it was manually searched, consistent with his training and practice.

requisite nexus showing between purported unconstitutional searches and the challenged evidence.

First, in addition to the photographs of the artifacts from the manual search, the search warrant affidavit included the following: (1) HSI had been investigating the defendant for artifacts smuggling prior to his arrival in the United States; (2) the defendant attempted to smuggle over 500 artifacts that smelled of wet earth and were covered in sand into the United States on the day his cell phone was seized; (3) the defendant made false statements to law enforcement about the goods he was bringing into the United States and his historic sales of artifacts; (4) the defendant had sold artifacts historically and created fake provenances; as well as (5) Special Agent Gamza's opinion, based on his training and experience, that artifacts looters communicate using cell phones.

Given the totality of these circumstances, even if this Court excised the photographs from the manual search, there was probable cause that evidence of the defendant's smuggling would be found on the only phone in his possession after his arrival in the United States from Egypt with contraband in tow. United States v. Singh, 390 F.3d 168, 182 (2d Cir. 2004) (citations and internal quotation marks omitted) ("A showing of nexus does not require direct evidence and may be based on reasonable inference from the facts presented based on common sense and experience."); see also United States v. Kenneth Ukhuebor, No. 20-MJ-1155 (LDH), ECF No. 24 at 4–9 (Mar. 19, 2021 Mem. & Order) (denying motion to quash, crediting agent's training and experience in probable cause determination and noting that doubts as to probable cause should be resolved in favor of upholding the warrant); United States v. Elgin Brack, No. 18-CR-684 (ENV), ECF No. 122 at 8–9 (Jan. 16, 2020 Mem. & Order) (denying defendant's motion to suppress cell phone and citing cases where statements in warrant affidavits linking the use of a cell phone with illegal activity based on an agent's training and experience, in conjunction with a description of the facts linking the defendant to the criminal activity, were sufficient to establish probable cause for a search of that defendant's cell phone); United States v. Barret, 824 F. Supp. 2d 419, 448–49 (E.D.N.Y. 2011) (denying motion to suppress and finding probable cause to search a cell phone based on the agent's statements in warrant affidavit about the capability of cell phones to store information and her experience that cell phones are used to further criminal activity).

Further, to the extent that the Court concludes that the photos should be excised from the warrant and that there was not probable cause for it to issue without them, the good faith exception to the exclusionary rule would still prevent suppression, as it is applicable even where a search warrant affidavit contains illegally obtained evidence. See United States v. Ganas, 824 F.3d 199, 225 (2d Cir. 2016) (en banc) (applying the good-faith doctrine to the subsequent warrant-authorized search, even though the affidavit contained evidence obtained in violation of the Fourth Amendment, because the officer was acting in good faith and had no reason to believe that his actions were unlawful).

Second, even if the Court were to find the defendant's reliance on United States v. Laynes, 481 F. Supp. 3d 657 (S.D. Ohio 2020)—an out of circuit district court decision issued after the search in this case—persuasive, at most it would mandate excision of the photos from

the search warrant affidavit; it would not require suppression of the warrant wholesale or bar the operation of the good faith exception to the exclusionary rule.

In Laynes, the court suppressed the defendant's cell phone because Google Photos—the sole application law enforcement manually searched prior to conducting subsequent searches—was utilizing cloud-based storage at the time of the manual search, as was noted by one officer who observed that the phone was *not* in airplane mode during the search and another who observed that the original child pornography video viewed on Google Photos was not accessible when the phone was in airplane mode. The court found that subsequent searches of the phone would not have been conducted but for the discovery of child pornography in the Google Photos application. Laynes, 481 F. Supp. 3d at 662, 667. Notably, law enforcement never obtained a search warrant for the phone and instead relied only on the border search for the evidence's admissibility. Here, by contrast, HSI was investigating an active artifacts smuggler and would have sought to forensically search the phone regardless of whether photos depicting looting were discovered during a manual search either through a warrant or the border search authority.

Moreover, it is unclear what, if any, constitutional import a violation of CBP internal policy that is not law and confers no private right of action on a passenger has, especially as the policy states that “Officers may not *intentionally* use the device to access information that is stored remotely. To avoid retrieving or accessing information stored remotely and not otherwise present on the device, Officers will either request that the traveler disable connectivity to any network (e.g., by placing the device in airplane mode), or, where warranted by national security, law enforcement, officer safety, or other operational considerations, Officers will themselves disable network connectivity.” CBP Directive 3340-049A at ¶ 5.1.2 (emphasis added), available at https://www.dhs.gov/sites/default/files/publications/CBP%20Directive%203340-049A_Border-Search-of-Electronic-Media.pdf (Jan. 4, 2018). As articulated by the Supreme Court, the principles underlying the border search exception include discovering contraband and preventing and disrupting its introduction into the United States. See Montoya de Hernandez, 473 U.S. at 537; United States v. Aigbekaen, 943 F.3d 713, 721 (4th Cir. 2019) (purposes of the border search exception include “disrupting efforts to export or import contraband”). Here, the defendant has made no showing that law enforcement's cursory review of his phone's camera roll after finding stolen antiquities and other evidence of smuggling in his luggage was anything other than reasonable, let alone that law enforcement intentionally used the defendant's phone to access photos that may have been stored in a remote server or cloud.

Third, for exclusion to be a proper remedy, the defendant is required to show that the challenged evidence was the fruit of the purportedly illegal search of remotely stored photos. See United States v. Marasco, 487 F.3d 543, 547 (8th Cir. 2007) (“the defendant bears the initial burden of establishing the factual nexus between the constitutional violation and the challenged evidence”). As the Supreme Court has emphasized, “[e]xclusion may not be premised on the mere fact that a constitutional violation was a ‘but-for’ cause of obtaining evidence.” Hudson v. Michigan, 547 U.S. 586, 592 (2006). Instead, only evidence “come at by exploitation of that illegality” is considered fruit of the poisonous tree. Wong Sun v. United States, 371 U.S. 471, 488 (1963).

Even if the facts are as the defendant says and search of the photo roll was not done in airplane mode and the phone was forensically searched prior to obtaining a warrant—and these searches are unconstitutional—the defendant has not established a factual nexus between the alleged constitutional violation and evidence obtained from either the search warrant or a forensic border search. And as noted above, no court has ever required more than reasonable suspicion for a full forensic search of electronics at the border, and some courts have allowed such searches with no suspicion whatsoever. There is simply no prejudice to the defendant over a cursory review of photos on his phone’s camera roll that may have been stored externally or via cloud computing when law enforcement had reasonable suspicion and probable cause for its forensic review (the act of which disconnects the device from cellular, Wi-Fi and Bluetooth connections).

Law enforcement’s right to conduct routine suspicionless border searches and non-routine searches supported by reasonable suspicion is clearly established in the Second Circuit. At the time the defendant’s phone was searched at the border, no court had ever addressed, much less held as dispositive, a phone not being in airplane mode as a factor in suppressing evidence. Above all, law enforcement’s actions were reasonable at each step: they performed a limited, cursory examination of the phone at the border after finding stolen antiquities and evidence thereof in the defendant’s luggage, applied for a warrant for its forensic search in an abundance of caution even though no court had ever held that a warrant was so required, and relied on that warrant in good faith. Accordingly, even assuming that the phone was not in airplane mode at the time it was manually searched, suppression is not warranted.

III. There Was No Discovery “Mix-up”

In his opposition, the defendant asserts that there was a “mix-up” in discovery that resulted in him receiving the forensic extraction of the phone on April 7, 2021. Def. Op. at 2. There was no mix-up on the government’s end. On August 18, 2020, the government asked defense counsel if he would prefer to receive Rule 16 discovery via a physical CD or via USAfx, a temporary file transfer program which deletes uploaded files after 60 days. Defense counsel requested USAfx. On August 21, 2020, the government made its first Rule 16 production, which included the forensic extraction of the phone and a Cellebrite reader, to the defendant via USAfx, notified the defendant of the production via ECF and email that day and asked defense counsel to inform the government if there were any issues accessing the discovery. See ECF No. 12. On April 5, 2021, defense counsel informed the government that he did not have the forensic extraction of the phone or the reader to view its contents and that they were not on USAfx. The government informed defense counsel that the files delete after a certain period and produced a second copy of the phone extraction and reader on April 6, 2021.⁴

Thus, there was no delay or mix-up by the government. The government produced the information to the defendant in August 2020, and defense counsel, after failing to

⁴ In its opening motion, the government stated that it reproduced the phone extraction on April 5, 2021. Upon review of the discovery emails in the case, the government notes that it started the production on April 5 but, given the size of the file, it was not reproduced until April 6, 2021.

download that information for at least sixty days, waited nearly eight months to request the information again. The defendant now requests supplemental discovery on the phone and its extraction six months after he filed his opening motion—over a year after the phone was initially produced—and attempts to improperly shift the burden to the government on issues on which the defendant has not even attempted to make a threshold showing as is required in a defendant’s motion to suppress. The defendant had every opportunity to investigate the issues he claims bear on suppression prior to the filing of his motion. Accordingly, in addition to not being outcome determinative, forensic expert testimony at this juncture would amount to a fishing expedition on theoretical Fourth Amendment violations of which the defendant has made no *prima facie* showing. United States v. Peeples, 962 F.3d 677, 692–93 & n.5 (2d Cir. 2020) (mere speculative belief that Fourth Amendment rights were violated is insufficient for defendant to meet burden in a motion to suppress, which requires motion and proof).

IV. The Defendant Was Not in Custody When He Disclosed His Passcodes and Thus No Fifth Amendment Violation Occurred

The defendant’s affidavit asserts that CBP took his cell phone and told him to unlock it. Def. Aff. ¶ 3. He refused but unlocked it with his fingerprint after he was told he had no choice. Id. CBP then asked for the phone’s passcode. Id. ¶ 4. The defendant asserts that he refused but complied when told he had to. Id. Notably, the defendant does not allege that he was handcuffed, arrested, had weapons drawn on him or was otherwise in custody in any objective terms. Indeed, the defendant attempts to elide the fact that this interaction occurred at a border, the purpose of which was to determine whether he and his effects were admissible into the United States, and thus some degree of questioning inheres in such situations; and that it occurred while CBP was recovering evidence of his illegal activity. United States v. FNU LNU, 653 F.3d 144, 153–54 (2d Cir. 2011); CBP Directive 3340-049A at ¶ 5.3.1 (“Travelers are obligated to present electronic devices and the information contained therein in a condition that allows inspection of the device and its contents.”).

In this context, even if the facts are as the defendant contends, his affidavit and motion describe nothing more than a modern border inspection, which is borne out by the JFK Airport footage depicting the defendant’s interactions with law enforcement that the government produced to the defendant. See United States v. Jean Carlo Mano, No. 18-CR-367 (WFK), ECF No. 26 at 18 (May 9, 2019 Decision & Order) (CBP officer’s “request for Defendant’s passcodes was relevant to Defendant’s admissibility into this country, as customs and border patrol authorities ask questions of thousands of passengers daily to ascertain whether they have attempted to bring contraband into the United States from abroad”). Because the defendant has made no showing that he was interrogated or in custody, Miranda warnings were not required prior to disclosing his passcodes, assuming that a biometric fingerprint unlock constitutes a statement for the purposes of the Fifth Amendment protection.⁵

⁵ To qualify for the Fifth Amendment privilege, a communication must be testimonial, incriminating and compelled. Hiibel v. Sixth Jud. Dist. Court of Nevada, Humboldt Cty., 542 U.S. 177, 189 (2004). The Supreme Court has long held that fingerprints are not testimonial, finding that the Fifth Amendment “offers no protection against compulsion to submit to fingerprinting.” Schmerber v. California, 384 U.S. 757, 764 (1966). Compelling a person to

Moreover, even if the defendant's passcodes were suppressed as self-incriminating statements made in violation of Miranda while in custody, suppression of the phone does not follow. In an abundance of caution, law enforcement obtained a search warrant authorizing a forensic review of the defendant's phone. Notably, the defendant does not contend that the his passcodes were relevant to the probable cause set forth in the search warrant affidavit or law enforcement's decision to seek a warrant at all. Accordingly, assuming CBP violated Miranda, the violation cannot infect the ensuing warrant. See Murray v. United States, 487 U.S. 533, 542 n.3 (1988) ("[W]hat counts is whether the actual illegal search had any effect in producing the warrant, not whether some hypothetical illegal search would have aborted the warrant. Only that much is needed to assure that what comes before the court is not the product of illegality; to go further than that would be to expand our existing exclusionary rule."); Wong Sun, 371 U.S. at 488.

V. Conclusion

For the reasons set forth herein, the Court should preclude the defendant's expert from testifying at the evidentiary hearing scheduled in this case.

Respectfully submitted,

JACQUELYN M. KASULIS
Acting United States Attorney

By: /s/
Marietou Diouf
Assistant U.S. Attorney
(718) 254-6263

cc: Clerk of the Court (LDH) (by ECF and Email)
Kannan Sundaram, Esq. (by ECF and Email)

provide a physical feature does not render the act testimonial simply because incriminating inferences might be drawn or that doing so may help lead the government to incriminating evidence. Doe v. United States, 487 U.S. 201, 208–09 & n.6 (1988).